## REMARKS

Applicant has carefully studied the outstanding Office Action in the present application. The present response is intended to be fully responsive to all points of rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application are respectfully requested.

Claims 36-39 stand rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement.

Concerning the above rejection, the Examiner wrote "Learning only the normal behavior of the application is ... not described in the specification." The applicant respectfully submits that the language of claims 36-39 is supported in the specification by page 6, second paragraph, taken in conjunction with page 9, lines 11 - 17. Specifically, the second paragraph of page 6 states (emphasis added):

"The present invention is thus operable to provide sets of parameters in which each individual program is allowed to operate. In order to determine whether a particular application is operating **normally,** embodiments of the present invention use, or create and use, a listing of activities that the application may wish to carry out. This listing is alternatively referred to herein as the application's predefined set. The activities are either permitted or forbidden, depending on whether they are part of the predefined set. The listing may be used to validate operations that the program tries to carry out. If the operation is not one that the listing permits then either the user is alerted to give specific permission or the operation is stopped altogether."

In summary, the second paragraph of page 6 teaches that normal behavior is associated with a set of permitted activities. Page 9, lines 11-17 describe the substance and duration of the learn mode (emphasis added):

"In the event that an enforcement file is not available, an embodiment of the invention, whose flow diagram is shown in Figure 2, has a so-called **learn mode 21**. In this mode a new program is assigned a general enforcement file. The general enforcement file gives the program no access rights at all to files on the system disk. The program then attempts to make a file access 20. Provided the attempt is within certain parameters the system allows the attempt and **learns** the details 23 so that in future an access to that area of the disk will always be allowed. Thus a specific enforcement file is gradually built up over the **duration** of the **learn mode**."

Applicant respectfully submits that the above two portions of the specification, taken together, support the language of claim 36 ("only normal accesses of said application ... are monitored during said limited time period"), of claims 37 - 38 ("said apparatus for learning about the program is for learning about only the normal access behavior of the program during said learning period") and claim 39 ("said monitoring ... learns only the normal behavior of said application"). Accordingly, claims 36-39 are deemed allowable.

Claims 19 and 21-39 stand rejected under 35 USC 103(a) as being unpatentable over Shieh et al (US 5,278,901, hereinafter Shieh) in view of Crosbie et al. In the Response to Arguments section, the Examiner takes the position that "Shieh teaches not only detection but also penetration resistance necessary to prevent illegitimate access (col. 1, lines 17 - 19). In addition, Crosbie ... teaches responding to an intrusion -- once an intrusion is detected, how is it dealt with (page 4, lines 21 - 22).

Col. 1, lines 17 - 19 of Shieh states: "In principle, access control and authentication mechanisms can provide the penetration resistance necessary to prevent illegitimate access by unauthorized users."

Page 4, lines 21 - 22 of Crosbie states: "A system by Kephard takes a similar approach to this paper.... his paper describes some issues that must be addressed by our system. These include...response to an intrusion - once an intrusion is detected, how it is dealt with."

Applicant respectfully points out that, as for the citation from Shieh, Shieh does indeed teach that "in principle" access control and authentication mechanisms "can provide the penetration resistance necessary to prevent illegitimate access," however, he immediately goes on to say (col. 1, lines 20 - 24) that "intrusion resulting from operational security problems can be prevented by neither authentication nor access control ... Instead, this type of intrusion must be detected by after-the-fact analysis of audit trails." The citation from Crosbie merely refers to "dealing with" a detected intrusion and does not specifically show or suggest actual prevention or restriction of the detected abnormal behavior, as in the claims of record.

In view of the above discussion, independent claims 19, 22, 24 and 25 are deemed allowable. Claims 21, 23, 26 - 39 depend from these claims and recite additional patentable subject matter and are also deemed allowable.

Applicant has also amended claims 24 and 39 to more clearly define the present invention.

Applicant had also added new independent claims 40-41, which have been annotated below to indicate their relationship to independent claims 19 and 25 respectively:

40. Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about the normal access behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to elements of said data storage during a limited period; and

an enforcement device, operative after said period is over, for [identifying and preventing said application from accessing elements of data storage that do not correspond with the normal behavior of said application] granting said application no access rights to any elements of data storage other than those elements accessed during said limited period, to which access will be allowed.

41. A method for detecting abnormal behavior of a first application executed on a computer system, and preventing the damage thereupon, comprising:

monitoring accesses of said application to elements of data storage arranged sectorwise in a storage device over a limited period of time and storing information about said accesses in an enforcement file, thereby learning the normal behavior of said application; and

when said period is over, [detecting attempts of said application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon] granting said application no access rights to any elements of data storage other than those elements accessed during said limited period, to which access will be allowed.

Support for new claims 40 and 41 is found in the specification on page 9, lines 11 - 17, which states that: "an embodiment of the invention...has a so-called learn mode. In this mode a new program is assigned a general enforcement file. The general enforcement file gives the program no access rights at all to files on the system disk. The program then attempts to make a file access 20. Provided that the attempt is within certain parameters the system allows the attempt and learns the details 23 so that in future an access to that area of the disk will always be allowed. Thus a specific enforcement file is gradually built up over the duration of the learn mode".

Applicant respectfully submits that new claims 40 and 41 are not anticipated by any of the prior art of record. Crosbie states, on page 6, that "a group of free-running processes...termed Autonomous Agents... will be trained to detect anomalous activity in (the network) traffic (on a system) by being subjected to a training phase by a human operator. The operator will present different styles of network traffic (both intrusive traffic and neutral traffic) and guide the learning of the agents. Note that the agents use Genetic Programming to actually learn." In other words, in contrast to the invention recited in claim 41, access is not necessarily allowed, after the training or learning period, to elements accessed during that period, according to Crosbie, because some of the elements accessed during that period admittedly constitute "intrusive traffic" i.e. their access is to be prevented, rather than allowed, at future opportunities.

Shieh clearly does not necessarily allow access, after the training or learning period, to elements accessed during that period, because Shieh takes into account presence of "Trojan horses" which may be present and active during the training or learning period and nonetheless, of course, should not be entitled to access. Shieh states "This approach has the advantage of detecting ... Trojan Horses" (Abstract).

Applicant has also added new claims 42-44. The present invention is directed to ensuring that a program application operates normally as recited in claim 42. Support for claim 42 is found in the specification on page 6, lines 12-23.

Applicant respectfully submits that at the time the invention was made it was common to block attempts of a user to access elements of data storage of another user. For example, on mainframe computers that serve a plurality of users, a user was not allowed to access files of another user. The innovative and inventive step of the present invention is that a program is prevented from accessing elements of data storage that the program is not supposed to access, in contrary to the prior art approach in which the focus was on the user. Thus, according to the prior art approach, as long as a user's program accesses data storage of said user, its attempts are legitimate, and therefore it cannot be used for blocking viruses.

Support for new claim 43 is found in Fig. 2 and the description thereof. New claim 44 is supported in Fig. 3 and the description thereof. Applicant respectfully submits that the invention claimed in claims 42-44 is not shown or suggested by the prior art.

Applicant reserves the right to pursue the claims as originally filed in the context of a continuation application.

In view of the foregoing, all of the claims are deemed to be allowable. Favorable reconsideration and allowance of the application is respectfully requested.

Respectfully submitted,

Christopher [illegible]

Reg No. 41,533